UNITED STATES DISTRICT COURT EASTERN DISTRICT OF VIRGINIA
Alexandria Division

DeShawn Deane, *on behalf of himself and all others similarly situated*,

Plaintiff,

vs.

Capital One Financial Corporation,

Defendant.

JURY TRIAL DEMANDED

Case No. 1:23-cv-556

CLASS ACTION COMPLAINT

1. Plaintiff DeShawn Deane ("Plaintiff") hereby files this Class Action Complaint against Defendant Capital One Financial Corporation. (hereinafter "Capital One" or "Defendant"), on behalf of himself and all others similarly situated. Plaintiff brings this action based upon personal knowledge of the facts pertaining to himself, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

I. NATURE OF THE ACTION

2. Capital One along with six of the nation's other large banks, created "Zelle" – an electronic payment system to compete with the wildly popular consumer payment systems such as PayPal, Venmo, and CashApp. In order to encourage and expand the use of Zelle, after it launched in 2017, Capital One began embedding Zelle into every customer's online account, and aggressively advertised it to its customers as "safe," "secure," and "easy." And in a further attempt to differentiate Zelle from its competitors, Capital One and Zelle contended it offered faster payments between bank accounts, allowing the transaction to occur within seconds, while Zelle

also advertised it as safe and secure because it was "backed by the banks."

3. Defendant's efforts have been extraordinarily effective. Zelle is now the single most popular such platform in the U.S., processing more money than Venmo and CashApp combined.[1] But Zelle is neither safe nor secure. In fact, it is a favorite mechanism for criminals and fraudsters to steal money from Capital One customers for the very same reasons that Capital One was able to effectively encourage its customer base to rapidly adopt it. For, unlike other peer-to-peer payment apps such as Venmo, Zelle is already integrated in the customer's online banking app and automatically connected to their bank account. Criminals can quickly, clandestinely and irreversibly move money out of the Capital One account once they gain access to it. As noted by Senator Elizabeth Warren, Capital One and its cohorts "created the perfect weapon for criminals to use, and they have used it."[2]

4. Fraud that victimizes Capital One's own customers through Zelle generally comes in two forms: 1) activity in which a user's checking and/or savings account is accessed by a bad actor and used to transfer a payment to another account controlled by the fraudster – referred to as "unauthorized" transactions – and 2) activity in which a user is fraudulently induced into transferring a payment to a bad actor – often referred to by Capital One as "authorized" transactions.

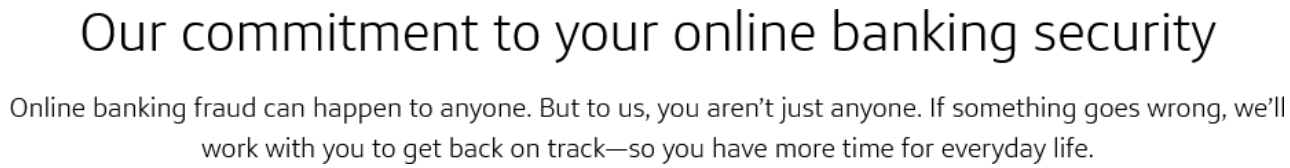
5. Capital One is of course aware that its customers are losing tens of millions of dollars every year due specifically to ***unauthorized*** transactions via Zelle. But, Capital One does nothing, in large part because Capital One has an enormous financial incentive to push Zelle on its customers

[1] *Forbes*, "Despite A Late Start, Bank-Owned Zelle Moves More Money Than Venmo and Cash App Combined," Emily Mason, September 8, 2022, available at: https://www.forbes.com/sites/emilymason/2022/09/08/despite-a-late-start-bank-owned-zelle-moves-more-money-than-venmo-and-cash-app-combined/?sh=7c175ed89d3f (last accessed November 4, 2022).
[2] Senate Report, Facilitating Fraud: How Consumers Defrauded on Zelle are Left High and Dry by the Banks that Created It, By Senator Warren, October 2022.

and encourage them to use it. First, Capital One is a controlling bank with an ownership stake in Zelle and profits through Zelle. Second, Capital One saves millions of dollars by avoiding paying transaction fees to other competing networks. Third, Capital One saves millions of dollars by reducing the amount of checks and cash transactions it is required to process. Last, Capital One saves tens of millions every year by unlawfully refusing to reimburse consumers for unauthorized transactions.

6. Although Capital One knows otherwise, it advertises its online and mobile banking as "safe" and "secure," and never discloses to its customers that Capital One subjected each and every one of them to a high risk of fraud for unauthorized transactions by embedding Zelle into each user's account.

7. Capital One promised its customers online banking security and protection from fraud.[3]



8. But Capital One does not protect their customers from unauthorized Zelle transactions. In fact, Capital One created the perfect weapon for criminals to steal money from its customers and does nothing to help when 'something goes wrong.'

9. Victims of unauthorized transactions via Zelle, like Plaintiff here, are left devasted after losing hundreds or thousands of dollars each time it occurs. For many customers, that money is needed to pay for rent, groceries, medicine or other necessities. Nonetheless, Capital One refuses to help their customers when criminals do steal money from their accounts – in spite of its promises

[3] https://www.capitalone.com/bank/security-fraud-protection/

and an undeniable legal obligation to do so.

10. Capital One is legally obligated to reimburse its customers for these losses from unauthorized transactions. For theft resulting from unauthorized transactions, the burden rests squarely on the shoulders of Capital One to conduct a reasonable investigation of the theft and either a) reimburse their customers or b) satisfy its own burden of showing that the customer's loss was not the result of an "Unauthorized Transfer."[4] But as a matter of company-wide policy and practice, Capital one does neither. Instead, it places the burden on its own customers – who are victims of the fraud – and refuses to reimburse them unless the consumer can prove to Capital One's satisfaction that the loss qualifies as an Unauthorized Transaction. And even then, in many cases Capital One still refuses to reimburse its customers.

II. JURISDICTION

11. The Court enjoys original subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because this case arises out of violations of federal law under the EFTA, 15 U.S.C. §§ 1693, *et seq*. Jurisdiction of this Court arises pursuant to 28 U.S.C. §§ 1331 and 1367 for supplemental jurisdiction over the state law claims asserted herein.

12. The Court also has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because (i) there is minimal diversity; (ii) Defendant is not a government entity against whom the District Court may be foreclosed from ordering relief; (iii) there are more than one hundred (100) people in the putative classes; and (iv) the amount in controversy exceeds $5,000,000, including attorneys' fees but exclusive of interest and costs.

III. VENUE

13. Venue in this District is proper pursuant to 28 U.S.C. § 1391(b) because Defendant

[4] See, generally, 15 U.S.C. §§ 1693*, et seq.* and 12 CFR Part 1005 (Regulation E).

has its headquarters in this district, Defendant transacts business within this judicial district and at all times relevant to these claims, a substantial part of the conduct and events giving rise the causes of action against Defendant occurred in this district. Defendant's account agreement contains a venue selection clause for the Eastern District of Virginia.

IV. PARTIES AND NON-PARTY

14. Plaintiff DeShawn Deane is a Texas citizen and resides in Fort Worth, Texas. He has been a Capital One customer for several years. He continues to maintain a personal checking account with Defendant.

15. On or about September 2, 2022, Plaintiff was attempting to set up advertisements on Facebook for his business. Plaintiff searched online and called a phone number that appeared to be the Facebook technical support line. Plaintiff unwittingly ended up communicating with a fraudster who was impersonating Facebook support. Plaintiff believed he was speaking with an Facebook representative.

16. The fraudster deceived Plaintiff into downloading an app on his iPhone called 'AnyDesk' which provided the fraudster control of his iPhone. Thereafter, the fraudster was able to send money from Plaintiff's Capital One account through Zelle. The fraudster told Plaintiff that he was simply linked his Capital One account to set up the Facebook advertisements. Plaintiff did not initiate the transaction or authorize it in any way. Plaintiff had never heard of Zelle.

17. Plaintiff immediately called Capital One to report the unauthorized transaction and fraud. Capital One denied Plaintiff's claim. Capital One did not provide Plaintiff with the evidence Capital One relied upon to reach its conclusion. Nor did Capital One provisionally credit his account after ten days of the Plaintiff filing the claim.

18. Defendant Capital One Financial Corporation ("Capital One") purports to be a large

diversified financial services holding company, including banks. According to its most recently-filed SEC Form 10-K (for FY 2021), Capital One is incorporated in Delaware and maintains its principle executive offices in McLean, Virginia. Much of the conduct complained of herein, including the adoption and implementation of certain policies and procedures, originated or took place at the corporate headquarters in Virginia.

19. Non-Party Early Warning Services, LLC ("Early Warning") is a privately-held financial services company owned and controlled by Capitol One, Bank of America, JPMorgan Chase, PNC Bank, US Bank, Wells Fargo, and Truist. Its principal asset is "Zelle." Zelle is a money payment platform ("MPP"). Zelle is incorporated into Capital One's online and mobile banking platform and is designed to facilitate and execute peer-to-peer instant payment services.

V. FACTUAL ALLEGATIONS

A. The Rise of Peer-to-Peer Payments

20. Peer-to-peer ("P2P") payment systems, also known as money transfer apps, allow users to send and receive money from their mobile devices through a linked bank account or credit or debit card. Examples of popular P2P systems include PayPal, Venmo, Google Pay, and CashApp.

21. In the past, sending money meant using cash, mailing a check, initiating a bank or "wire" transfer, or using a debit or credit card. All of these situations were inconvenient, expensive or took time for the recipient to actually receive the money in their bank account. And they cost both the sending and receiving bank money (as well as the parties, sometimes) because each participating bank had to process these transactions.

22. With P2P payments, users can quickly send funds while keeping their bank account details private. Usually, all that is required to make a P2P payment is the recipient's username,

email, or phone number. For example, if two persons want to split a restaurant bill at the time of payment, one person can simply take out their phone, open the app, type the amount to send, enter the recipient's phone or email to find his/her account, and hit send. The money is instantly transferred and there is no processing fee. These app-based payment systems are very popular for sending money between friends to split a check, pitch in for gifts, as payment for rent to landlords, and to pay for services at the time they are performed.

23. Although P2P transactions have exploded over the past few years, P2P payments are nothing new. Venmo hit the market in 2009 as a P2P payment service and was acquired by PayPal in 2013. Venmo in particular has gained huge popularity since 2015, especially with consumers between the ages of 18-35.

24. Venmo generally does not charge users for sending or receiving money and initially was frequently used to split tabs among friends or share roommate expenses like rent and utility bills. In order to send or receive money through Venmo, users had to download an app, create an account, and link it to a bank card or banking account. Venmo initially limited the transactions to a maximum of $299 until the user verified his/her identity.

25. App use for transferring money and making payments has skyrocketed in the last 10 years. In 2016, Venmo processed over $17 billion in payments and processed almost $7 billion in the first quarter of 2017. Zelle's growth continues, rising to $490 billion in payments in 2021, more than double Venmo's P2P volume.[5] Zelle has transferred $1.5 trillion since 2017.

B. Zelle Is Created And Marketed To Compete With P2P Systems

26. To compete with Venmo and other P2P apps, a consortium of the largest banks

[5] *American Banker*, "Can Zelle change the narrative around P2P fraud?, Kate Fitzgerald, March 9, 2022, available at: https://www.americanbanker.com/payments/news/can-zelle-change-the-narrative-around-p2p-fraud (last accessed November 4, 2022).

teamed up to launch their own money transfer app called "Zelle." While Zelle is owned by Early Warning Service ("EWS"), EWS is owned, operated, and controlled by seven of the largest banks in this country, including Defendant Capital One.

27. Launched in June 2017, Zelle lets banks handle electronic transfers without paying any fees to third parties.

28. With Venmo and other P2P apps gaining so much popularity, Zelle and Capital One recognized that it would be difficult to compete with Venmo, et al., and convince users to switch to using Zelle. Therefore, Zelle differentiated itself from Venmo by marketing Zelle as "faster" and "safer" than its competition. Zelle advertisements emphasized its security and safety, because it is "backed by the banks."[6]

29. For example, in a 2018 television commercial, Zelle hired performer Daveed Diggs from the Broadway show Hamilton to rap: "You can send money safely cause that's what it's for / It's backed by the banks so you know it's secure." In another commercial with Daveed Diggs, Zelle similarly advertised that is "safe" and "backed by the banks."[7]

30. Zelle's CEO also publicly touted its safety and faster payments. Zelle offers a "faster payments network that will revolutionize how U.S. consumers and businesses send and receive money" said Paul Finch, then CEO of EWS. He announced that Zelle "will change how money moves, empowering millions of consumers with a faster, safer way to send and receive payments within the security of their financial institution."[8]

---

[6] Tech Crunch, "Zelle p2p payments push to compete with Venmo now has 19 US FI backers" Natahsa Lomas, (October 24, 2016), available at: https://techcrunch.com/2016/10/24/zelle-p2p-payments-push-to-compete-with-venmo-now-has-19-us-fi-backers/ (last accessed November 4, 2022).

[7] WRAL News, "Zelle Fraud Protection: What You Need to know Before Transferring Funds" (May 1, 2018) available at: https://www.wral.com/zelle-fraud-protection-what-you-need-to-know-before-transferring-funds/17523584/ (last accessed November 4, 2022

[8] Zelle Press Release, October 24, 2016, available at: https://www.zellepay.com/press-releases/early-warning-announces-zelle-network (last accessed November 3, 2022).

31. Likewise, Lou Anne Alexander, group president of payments for Early Warning stated in an interview: "As I've said, Matt, consumers know two things about the way that they pay. They do not pay to pay, and it's really difficult to get consumers out of their current payment behavior. Just think about it -- you probably pay your landlord in the very same way; you probably pay for your groceries in a very different way than you pay your babysitter. As we're focusing on changing consumer behavior, we're having great success in helping customers understand that it can be fast, and it can be easy. But we also have to help them understand it also can be safe for them."[9]

32. To gain users, Zelle also marketed to an older demographic that may not be comfortable using Venmo due to safety or security concerns. Melissa Lowry, Early Warning's vice president of marketing and branding, stated they are targeting an older age demographic. She noted that "This group has a high trust in their banks," so Zelle "wants to remind these consumers that money transfer isn't just for splitting a restaurant tab, it can also be used for splitting a payment on kids' sports uniforms or grocery store bills," Lowry said. "That demographic had been a bit ignored in the (P2P) category." *Id.*

33. This marketing strategy worked by attracting an older demographic that trusted Capital One. "76% of Gen X and 74% of Baby Boomers also said that offered through their financial institution was the key reason that they would trial P2P payments." *Id.*

34. But Zelle is different from other digital payment systems such as PayPal, Google Pay, or Venmo in several important respects. ***First***, with Zelle, the transfer goes ***immediately*** from bank account to bank account – there is no entity holding onto the money while the transaction is verified or before it's collected by the recipient. Zelle doesn't hold

[9] Fox Business News, "Bank Earnings and Getting to Know Zelle" Matt Frankel, available at: https://www.foxbusiness.com/markets/bank-earnings-and-getting-to-know-zelle (last accessed November 4, 2022).

the money for any period of time. Instead, the money transfers immediately from a Capital One customer's bank account to the recipient's bank account.[10]

35. ***Second***, and unknown to many Capital One customers, Zelle is automatically integrated in the customers' Capital One account. This allows criminals to instantly transfer money via Zelle from Capital One customers, many of whom are not even aware of the Zelle feature embedded in their online accounts.

C. Unknown To Many Capital One Customers, Zelle Is Embedded In Their Accounts And "Always On" – It Cannot Be Removed Or Disabled

36. Capital One has embedded Zelle in each and every Capital One online and mobile account. It cannot be removed by the customer; nor can it be disabled. Zelle is directly embedded within mobile banking channels of its network banks and is "always on."[11]

37. Being integrated in the banking platform offered a big competitive advantage for Zelle. "There's no need to download an additional app, it's right there in the trusted financial institution, online banking or mobile banking app that I currently use."[12]

38. "One of Zelle's unique characteristics is that it is embedded within the online and mobile banking experience of individual network banks," said the spokesperson. "That means customers never have to leave the safety of their financial institution to make a payment. There is never a need for a customer to provide an account number to a third party app, which is one very effective way for Zelle users to protect their identity and payments."

39. Capital One does not offer customers a way to delete or disable the Zelle function.

---

[10] Los Angeles Times, Do you use Zelle? Here's how to spot increasingly common scams. (Oct. 7, 2022) Jon Healey, available at: https://www.latimes.com/business/technology/story/2022-10-07/zelle-banks-may-not-cover-the-losses-from-scams (last accessed Nov 3, 2022).

[11] Zelle Press Release, October 24, 2016. Available at: https://www.zellepay.com/press-releases/early-warning-announces-zelle-network (last accessed November 3, 2022).

[12] Bank Earnings and Getting to Know Zelle, April 17, 2019, available at: https://www.foxbusiness.com/markets/bank-earnings-and-getting-to-know-zelle (last accessed November 3, 2022).

Capital One does not provide any means, or instructions, on how to turn Zelle off or prevent fund transfers via Zelle. By design, Capital One customers simply cannot avoid the unauthorized transfers via Zelle even if they were aware of the risk.

D. Capital One and Zelle Make It Easy To Steal From Capital One Customer Accounts

40. Zelle and Capital One created the perfect weapon for criminals to use and they have used it. The National Consumer Law Center has described Zelle as "a dangerous payment system" and it has become the preferred tool for criminals.[13]

41. Because it is already embedded into the Capital One account, and the money transfer is immediate, criminals can easily and quickly transfer money out of a Capital One bank account. In fact, criminals have targeted Capital One customers precisely because Zelle is already integrated in their account and they can quickly and irreversibly move money out of the account once they gain access.[14] And it is costing Capital One customers millions of dollars.[15]

42. Nearly 18 million people have been victims of "widespread fraud" on money transfer apps, according to a letter sent in late April of 2022 to Zelle by U.S. Senators Elizabeth Warren of Massachusetts, Robert Menendez of New Jersey and Jack Reed of Rhode Island. Criminals have turned to Zelle as their favorite service because transfers are immediate and unrecoverable, and a fraudster can become a Zelle user (and money transfer recipient) without revealing their true identity.

---

[13] "95% of the shut-off scams requested payment through Zelle." Detroit Free Press "DTE Impersonators Drained Rochester Hills Woman's Checking Accounting Using Zelle App", Tompor, Susan (June 30, 2022),available at: https://www.freep.com/story/money/personal-finance/susan- tompor/2022/06/30/utility-shutoff-scam-stole-cash-via-zelle/7714138001/ (last accessed Sept. 21, 2022).

[14] NBC News, "Instant Fraud, Consumers See funds disappear in Zelle account scam" Vicky Nguyen, Did Martinez, Joe Enoch, and Michelle Tak (June 11, 2019) available at: https://www.nbcnews.com/business/consumer/instant-fraud-consumers-see-funds-disappear-zelle-account-scam-n1015736 (last accessed November 3, 2022).

[15] Senate Report, Facilitating Fraud: How Consumers Defrauded on Zelle are Left High and Dry by the Banks that Created It, By Senator Warren, October 2022.

43. Led by Idaho Attorney General Lawrence Wasden and Oregon Attorney General Ellen Rosenblum, a bipartisan coalition of thirty-three (33) attorneys general wrote the Consumer Financial Consumer Protection Bureau ("CFPB"), calling for stronger consumer safeguards for money sharing platforms and apps like Zelle. The letter, written in response to the CFPB's request for comments on its inquiry into "Big Tech Payment Platforms," noted a rise in complaints against popular payment apps including Zelle. The letter highlighted that: "[m]any consumers have been scammed out of hundreds or thousands of dollars by other users of these payment platforms [like Zelle]. Scammers are attracted to real-time payment platforms, in large part, because they do not need to reveal their true identity to set up an account" (emphasis added).[16]

44. Criminals can transfer money out of Capital One's customer accounts using Zelle by hacking their accounts or phones, obtaining access to their phone, tricking customers into providing their login information, or through robbery.

45. For example, rather than demanding your wallet, some criminals demand your phone, knowing that they can quickly and anonymously transfer money via Zelle. One such Capital One customer complained after he was robbed at gun point. The thief demanded his iPhone and passcode. The thief drained $8,294 from his bank accounts at Capital One via Zelle. Capital One only refunded $250, saying it found no evidence that the rest of the money was stolen. "I filed a police report, identified the suspect at a precinct, and even testified at a grand jury" the victim stated. "But none of that seems to have helped my case." Capital One refused to return his money, despite what appeared to be obvious unauthorized transactions. Only after being contacted by the *New York Times* did Capital One reimburse the victim as required by law and its own contract.[17]

---

[16] Attorneys General Letter dated December 20, 2021 to CFPB Director Rohit Chopra, regarding "Request for Comments Big Tech Payment Platforms" Docket No CFPB-2021-0017.

[17] When Customers Say Their Money Was Stolen on Zelle, Banks Often Refuse to Pay", The New York Times, Stacy Cowley and Lananh Nguyen (June 20,2022) available at:

46. Sometimes criminals use a phishing email or phone call that appears to be from Capital One itself, tricking consumers into entering their bank ID and password into a fraudulent website. Once a fraudster gains this information, they have unfettered access to transfer funds from the account immediately using Zelle.

47. And hackers have figured out how to defeat any text-message-based authentication for Zelle transfers. Either they trick victims into divulging authentication codes, in a phone call, or they intercept the messages electronically. In the past, criminals also have cloned phones, or simply changed the cell phone number associated with an account so the message is directed at a phone they control.[18]

48. Ken Otsuka, a senior risk consultant at CUNA Mutual Group, an insurance company that provides financial services gives an example of one such scam. Otsuka said a fraudster may call from a number spoofed to look like its coming from your bank, so suspicious customers will look up the number and believe it is indeed their bank calling. Next, the fraudster may inform you that there appear to be some fraudulent transactions on your account and ask: "Before I get into the details, I need to verify that I'm speaking to the right person. What's your username?" "In the background, they're using the username with the forgot password feature, and that's going to generate one of these two-factor authentication passcodes," Otsuka said. "Then the fraudster will say, 'I'm going to send you the password and you're going to read it back to me over the phone.'" The fraudster then uses the code to complete the password reset process, and then changes the victim's online banking password. The fraudster then has unfettered access to use Zelle

---

https://www.nytimes.com/2022/06/20/business/zelle-money-stolen-banks.html (last accessed 10/31/2022); "Fraud is Flourishing on Zell. The Bank Say It's Not Their Problem", The New York Times, Stacy Cowley and Lananh Nguyen, March 6, 2022, available at: https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html (last accessed October 31, 2022).

[18] Bob Sullivan, "Zelle Criminal took $23k from elderly victim" (August 26, 2019), available at: https://bobsullivan.net/cybercrime/zelle-criminal-took-23k-from-elderly-victim-bofa-initially-wouldnt-give-it-back/ (last accessed November 4, 2022).

to transfer the victim's funds.[19]

49. An important aspect of this scam is that ***the fraudsters never even need to know or phish the victim's password***. By sharing their username and reading back the one-time code sent to them via email, the victim is unwittingly allowing the fraudster to reset their online banking password. Normally, gaining access to your online account would not result in immediate financial harm. However, with Zelle embedded, the fraudster can immediately drain the bank account.

50. Many Capital One customers have never heard of Zelle and never knew that it was embedded into their account. Osaka noted that "Members don't have to request to use Zelle. It's just there, and with a lot of members targeted in these scams, although they'd legitimately enrolled in online banking, they'd never used Zelle before." *Id*.

E. Capital One Markets Its Mobile Banking Services As Safe and Secure

51. Capital One makes repeated promises on its website, app, and elsewhere that its online banking, which includes Zelle, is safe and secure.[20]

52. Capital One advertised its mobile app as "**quick, easy, and secure**" and promised on its mobile banking webpage that "**Capital One works hard to keep you and your money secure and protected against fraud**."

53. Capital One's website peddles the security and safety of its mobile banking and app to consumers. Capital One advertised that it provides "**secure banking**" and promises "**Your account is safe.**"

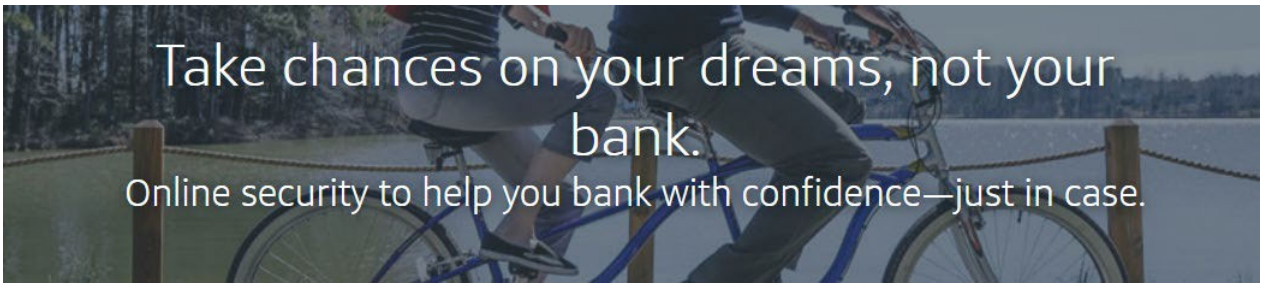
54. Capital One made promises of 'safety' and 'security' throughout its website and throughout the Class period, advertising that Capital One has "**safeguards to keep your account**

[19] The 'Zelle Fraud' Scam: How it works, How to fight back" November 19, 2021, https://krebsonsecurity.com/2021/11/the-zelle-fraud-scam-how-it-works-how-to-fight-back/comment-page-1/ (last accessed November 4, 2022).
[20] https://www.capitalone.com/help-center/checking-savings/transfer-funds-with-zelle/ (June 22, 2022).

secure'" "**Your security is our top priority,**" and "**your money is in a safe place**."[21]

55. To alleviate any concerns that consumers may have with the security of online banking, Capital One advertised that it would fight for their customers if any fraud should occur. "**An online banking security breach can happen to anyone, but to us, you aren't just anyone. Our fraud coverage means just that–we're in your corner. If something goes wrong, we'll work with you to get back on track and make things right**."

56. Capital One told customers that Capital One's online security allows them to bank online with confidence.



F. Capital One Does Not Disclose The Risks Posed By Zelle

57. Capital One knows that Zelle is not secure and that fraud and unauthorized transactions are overwhelming its own customers. Consumers began complaining about unauthorized transactions and money being stolen out of their accounts shortly after Zelle was launched and embedded into Capital One's customers' accounts in 2017.

58. By 2018, there were numerous news reports, including a *New York Times* report of Capital One customers losing money after being scammed or hacked through the use of Zelle.[22] And of course, Capital One gets tens of thousands of reports from its own customers every year, which it claims to "investigate."

[21] Checking & Savings - Bank Accounts | Capital One, available at: https://www.capitalone.com/bank/.
[22] See, e.g. https://www.nytimes.com/2018/04/22/business/zelle-banks-fraud.html ; See also, https://www.nbcdfw.com/news/local/consumers-say-their-bank-accounts-were-hacked-through-zelle/2054119/.

59. Capital One is also painfully aware that bad actors are routinely hacking into consumers accounts, phones, or tricking its customers into providing their account information and often setting set up the Zelle account embedded into each Capital One account to steal money.

60. But even after users complain about funds being stolen from their accounts through the embedded Zelle feature, Capital One frequently does nothing. Instead, Capital One continued to promote both its online banking as "secure" and "safe". Yet nowhere in Defendant's marketing do they warn potential Capital One customers of the risks of its online banking due to the incorporation of Zelle.

61. Consumers are often not aware of Zelle. And even if they know of it and use it, consumers are not aware that money transfer transactions with Zelle differ from other similar platforms. Unbeknownst to most Capital One users, the Zelle network has become a preferred tool for fraudsters to victimize Capital One customers.

62. In fact, due to the myriad security risks Zelle presents, security experts advise consumers not to use Zelle at all.[23] But Capital One does not offer a way for consumers to delete Zelle from their online banking account or mobile app in order to protect themselves.

63. "Scammers go where it's easy to get the money. Zelle is their current mechanism to drain consumer accounts," warned Ed Mierzwinski, PIRG Education Fund's senior director of federal consumer programs. "The scammers are taking advantage of consumers because the banks are letting them," Mierzwinski said. "My basic advice is don't use these apps." *Id.*

64. Capital One knows that Zelle creates a security risk and that Zelle is not safe or secure. Capital One also acknowledged that the "speed" of the Zelle app "gives online thieves

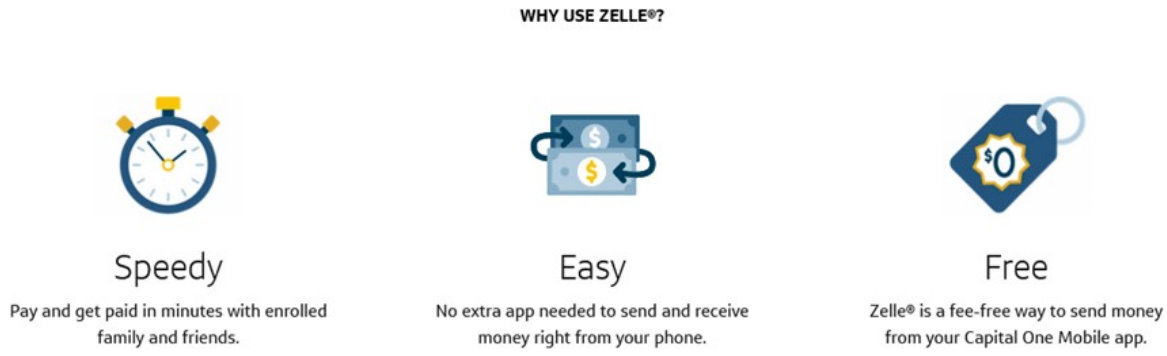
[23] Detroit Free Press "DTE Impersonators Drained Rochester Hills Woman's Checking Accounting Using Zelle App", Tompor, Susan (June 30, 2022),available at: https://www.freep.com/story/money/personal-finance/susan- tompor/2022/06/30/utility-shutoff-scam-stole-cash-via-zelle/7714138001/ (last accessed Sept. 21, 2022).

chances to take advantage of users who aren't paying attention."

65. In fact, Capital One recently stopped using the words **'safe'** and **'secure'** to describe Zelle on its website.

66. For the past few years, and until at least September of 2022, Capital One prominently described Zelle as secure, as seen in the advertisement below:

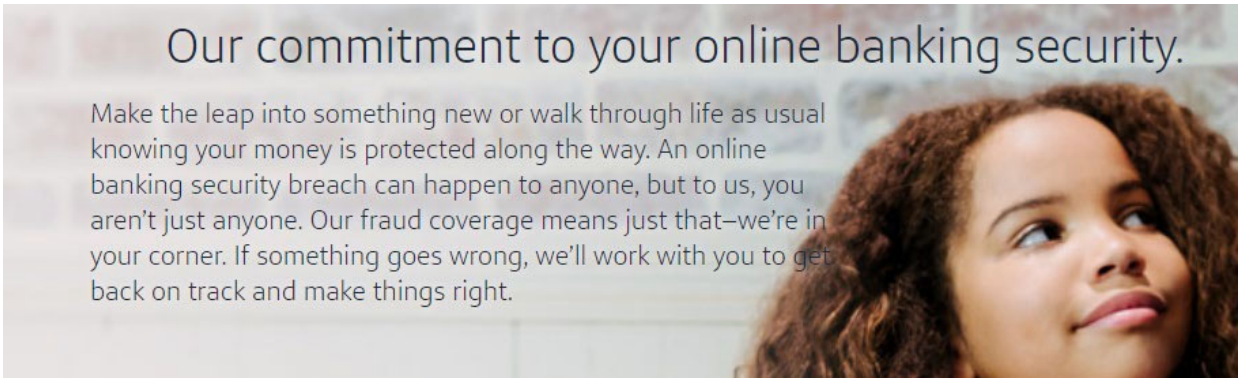
Now, Capital One only describes Zelle as "Speedy", "Easy", and "Free". Similarly, Capital One eliminated the words **"safe"** to describe Zelle through its website.



67. And while Capital One has changed its advertising, it still does not provide customers an option to delete Zelle or remove it from their own accounts. It remains automatically integrated in their mobile banking. Nowhere does Capital One warn its users of higher risk of fraud and scams by using Capital One's mobile banking, due to Zelle.

G. Capital One Specifically Promised Security, Protection And Reimbursement From Unauthorized Transfers

68. Capital One advertises a "commitment to your online banking security" and promised its customers that their money was protected and Capital One's fraud coverage would offer protection in case of a security breach:



69. Capital One is full of promises of security and statements like: "Capital One works hard to keep you and your money secure and protected against fraud."[24]

70. Elsewhere in describing fraud, Capital One promised: "**if something goes wrong, we'll work with you to back on track and make things right**."

71. Capital One prominently advertises that it provides "**$0 Fraud Liability**" and unequivocally assures its customers that: **"You're not responsible for unauthorized charges if your card is stolen."**[25]

[24] https://www.capitalone.com/bank/security-fraud-protection/ (last accessed November 16, 2022.
[25] https://www.capitalone.com/bank/security-fraud-protection/

72. Similarly, Zelle's website informs users that consumers should be able to get their money back from Capital One when they did not authorize the transaction**.**

73. Capital One's Checking Account Agreement also repeatedly promises users that, if they timely report fraud, that they will not be liable for fraudulent transfers. Only if the consumer does not promptly notify the bank and Capital One can prove that it could have stopped the unauthorized transfer had we been notified. Because the transfer is made within seconds and Zelle transactions cannot be stopped, this would never apply.

74. The checking account agreement provides that: and the Checking Account Agreement and Electronic Funds Transfer Statement (the "Agreement").

> If you notify us of the loss, your liability for unauthorized transfers will be as follows:
>
> A. **We have decided not to impose any liability on you even though the law says we could** (up to $50) if someone used your E-Identification without your permission and you contact us within two (2) business days after you learn of the loss or unauthorized use.
>
> B. If you do NOT tell us within two (2) business days and we can prove that we could have prevented the loss had you contacted us, you could lose as much as $500.00.

> C. If your statement shows transfers that you did not make and you do NOT contact us within sixty (60) days after the statement was made available to you, you may not get back any money lost after the sixty (60) days if we can prove that your contacting us would have prevented those losses.

(emphasis added).

75. Moreover, the terms provide that it will conduct a reasonable investigation if a consumer timely reports any errors (including unauthorized transfers) Capital One will credit the consumer's account within 10 days:

> We will tell you the results of our investigation within ten (10) business days after we hear from you and will correct any error promptly. If we need more time, however, we may take up to forty-five (45) (ninety (90) days for those transactions at merchant POS terminals, processing on a new account, or initiated outside the United States) to investigate your complaint or question. If we decide to do this, we will credit your account within ten (10) business days for the amount you think is in error, so that you will have use of the money during the time it takes us to complete our investigation.

76. Capital One acknowledges that there is a lot of fraud with Zelle and explains to its customers that scams and fraud are treated differently. Capital One promises that unauthorized transfers, like Plaintiff and Class Members experienced, would be refunded, but authorized transactions would not. Capital One explains the difference as follows:

> The terms scam and fraud are often used to mean the same thing. But there's a difference.
>
> In general, fraud happens when someone accesses or uses your account without your permission. Scams happen if you were tricked, but you were still the one who approved a payment. Basically, fraud involves unauthorized transactions. Scams involve authorized transactions.
>
> The difference is important, because the same protections aren't available if a transaction is authorized.

77. Capital One routinely violates each of these promises – and its legal obligations under the EFTA and Regulation E – as a matter of company policy.

H. Capital One Does Not Refund Customers For Unauthorized Transactions

78. Despite promising consumers that they won't be liable for unauthorized transactions, despite knowing that Zelle allows criminals to easily make unauthorized transfers out of customers' accounts, and notwithstanding that Capital One failed to notify consumers of this risk of Zelle and online banking, Capital One still refuses to refund its customers for unauthorized transactions resulting in part from Capital One's very own conduct.

79. Capital One's practices, policies and procedures do not comply with the promises made to customers, and they do not comply with Federal law.

80. Instead, Capital One has wrongfully denied its customers tens of millions of dollars in refunds for unauthorized transactions. On average, banks are refusing to refund over half of the unauthorized transactions. Capital One is likely worse, as it has refused to even provide this information to Congress, despite specific requests from the U. S. Senate.[26]

81. Capital One intentionally does not describe Zelle transactions in its Contracts, despite having Zelle integrated in the checking accounts since 2017. Moreover, Capital One intentionally does not provide an easy means to report Zelle fraud, instead leaving it to the consumer to figure out that it is considered an electronic funds transfer and how it should be reported. Capital One omitted describing Zelle to its customers in this way to deter complaints related to Zelle fraud.

I. Electronic Funds Transfer Act, 15 U.S.C. § 1693 *et seq.*

81. Capital One is required under the Electronic Fund Transfer Act to repay customers when funds are illegally taken out of their account without authorization.

82. Frequently, and as a matter of policy and practice, Capital One initially denies the claims for unauthorized transactions. After a denial, Capital One sometimes offers to "reopen the

[26] Senate Report, Facilitating Fraud: How Consumers Defrauded on Zelle are Left High and Dry by the Banks that Created It, By Senator Warren, October 2022.

dispute" after it was rejected, before Capital One considers refunding the stolen money.[27]

83. In enacting the EFTA, Congress found that the use of electronic systems to transfer funds provides the potential for substantial benefits to consumers. 15 U.S.C. § 1693(a). Congress' purpose in enacting the EFTA was to "provide a basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund and remittance transfer systems." Id. § 1693(b).

84. "The primary objective of [the EFTA] is the provision of individual consumer rights." *Id.* In response to the EFTA, the Federal Reserve Board of Governors passed Regulation E to implement that statute. Capital One and other banks are bound by the EFTA and Regulation E.

85. The EFTA and Regulation E apply to electronic fund transfers that authorize a financial institution to debit or credit a consumer's account. 12 C.F.R. § 1005.3(a). Recent CFPB guidance on ***unauthorized*** Electronic Fund Transfers ("EFTs") indicates P2P payments are EFTs, such that transactions made with Zelle will trigger "error resolution obligations" on Capital One to protect consumers from situations where they are fraudulently induced and requested by a third party to provide their account information that results in unauthorized debits from their accounts.[28]

86. Under the EFTA, an unauthorized electronic fund transfer is an electronic fund transfer from a consumer's account "initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit."

87. The Federal Deposit Insurance Corporation ("FDIC") issued a report in March 2022

---

[27] he New York Times, "Zelle, the Banks' Answer to Venmo, Proves Vulnerable to Fraud" Stacey Cowley, (April 22, 2018), https://www.nytimes.com/2018/04/22/business/zelle-banks-fraud.html.

[28] Consumer Financial Protection Bureau, Electronic Fund Transfers FAQs, https://www.consumerfinance.gov/compliance/compliance-resources/depositaccounts-resources/electronic-fund-transfers/electronic-fund-transfersfaqs/#financial-institutions-2 (last accessed October 28, 2022

finding that Regulation E's "liability protections for unauthorized transfers apply even if a consumer is deceived into giving someone their authorization credentials."[29]

88. Under Regulation E, if the consumer alleges that there has been an unauthorized transfer, the consumer's financial institution ***must*** investigate and determine if the allegation is true, correcting any unauthorized transfer that occurred. Reg. E, 12 C.F.R. § 1005.11(c)(1) [§ 205.11(c)(1)].

89. If a consumer alleges that an EFT is unauthorized, ***the burden of proof is on the financial institution*** to show that it was authorized or that the conditions for consumer liability have been met. But the extent of the consumer's liability is determined solely by the consumer's promptness in notifying the financial institution. "Other factors ***may not be used*** as a basis to hold consumers liable."[30]

90. Consumer negligence therefore plays no role in determining the consumer's maximum liability. An example of consumer negligence could be when someone writes a PIN on the debit card and there is an unauthorized EFT through use of the debit card. Despite the consumer's negligence, which facilitated the unauthorized electronic fund transfer, the consumer's liability is totally unaffected.[31]

91. The bank is also liable to the consumer if it does not conduct a good faith investigation of the claim, rejected the claim despite not having a reasonable basis to do so, or unreasonably failed to draw from the evidence that no error had occurred. 15 U.S.C. § 1693f(e).

92. The bank's efforts to investigate must be "reasonable" in light of available evidence

---

[29] FDIC, Consumer Compliance Supervisory Highlights Federal Deposit Insurance Corporation (March 2022), available at: https://www.fdic.gov/regulations/examinations/consumer-compliance-supervisory-highlights/documents/ccs-highlights-march2022.pdf (last accessed October 28, 2022)

[30] Reg. E, Official Interpretations § 1005.6(b)-3 [§ 205.6(b)-3]. Consumer Fin. Prot. Bureau, CFPB Consumer Laws and Regulations: Electronic Fund Transfer ACT 23 (Oct. 2013), available at www.consumerfinance.gov (CFPB Supervision and Examination Manual; original emphasis).

[31] Reg. E, Official Interpretations § 1005.6(b)-2 [§ 205.6(b)-2].

and the consumer's report of the error. The financial institution must review any relevant information within the institution's own records for the particular account." Although the extent of the investigation "may vary depending on the facts and circumstances . . . a financial institution may not limit its investigation solely to the payment instructions where additional information within its own records . . . could help to resolve a consumer's claim." The official interpretation includes a list of examples of the type of information that a financial institution might review, including "[a]ny other information appropriate to resolve the claim."[32]

93. Importantly, when there is an agreement between a third party and the banking institution, the bank ***must*** extend its investigation beyond its own records.[33] Here, Capital One has an agreement with Zelle and probably the recipient's bank to provide transactions via the Zelle network, and as a result Capital One is required to examine those third-party records during an investigation.

94. Capital One repeatedly and routinely fails to follow these mandatory requirements as a matter of practice and policy. For if Capital One conducted reasonable investigations, followed the evidence, and analyzed these records, it would see clear evidence of criminal activity and fraud and could not deny reimbursement of most of the unauthorized transactions it routinely denies.

95. Capital One determined that unauthorized transfers of funds via Zelle of Plaintiff and Class Members were not in error due to, at least in part, the Bank's financial self-interest as a stakeholder in Zelle, and to avoid its liability to Plaintiff and other Class members for the unauthorized transfers pursuant to Regulation E.

96. Bob Sullivan, a journalist and *New York Times* best seller, wrote: "I've since heard

[32] Reg. E, Official Interpretations § 1005.11(c)(4)-5 [§ 205.11(c)(4)-5].
[33] Reg. E, Official Interpretations § 205.11(c)(4), 12 C.F.R. § 205, Supp. I.

countless stories about victims getting the wrong advice from banks, who sometimes flat-out refuse to honor legitimate Regulation E disputes that should lead to consumers being "refunded" money stolen through unauthorized transfers. This story is important to me because it puts quite a human face on these victims. It gives me a chance to wonder why banks have gotten away with it so long, and why regulators haven't done more to fix this."

97. Capital One's practices and policies of denying a claim without performing a reasonable investigation are illustrated by Plaintiff's experience, as well as other instances in which the bank only investigated the claim after being contact by a news reporter.

98. Capital One created a system and adopted policies and procedures that treated Zelle transfers differently than other EFTs.[34]

99. Regulation E also requires the bank to report the results of its investigation to the consumer – which includes a written explanation of the institution's findings and the consumer's right to request the documents that the institution relied upon in making its determination.[35] As evidenced by the experiences of Plaintiff, Capital One does not comply with this obligation either.

100. When consumers notified Capital One about suspected errors regarding the Zelle transfers that were unauthorized, Capital One denied the claim without a reasonable investigation and did not state a reasonable basis for doing so. Moreover, Capital One did not provide a provisional credit the consumers account within 10 days as required.

V. CLASS ALLEGATIONS

101. Plaintiff brings this action on behalf of himself and on behalf of all other persons

[34] *See* fn. 41.

[35] Reg. E, 12 C.F.R. § 1005.11(d)(1) [§ 205.11(d)(1)]; Bisbey v. D.C. Nat'l Bank, 793 F.2d 315 (D.C. Cir. 1986) (bank liable when it provided oral explanation and did not inform consumer of right to request documents). Reg. E, Official Interpretations § 1005.11(d)(1)-1 [§ 205.11(d)(1)-1]. "If an institution relied on magnetic tape it must convert the applicable data into readable form, for example, by printing it and explaining any codes." *Id*.

similarly situated.

102. Plaintiff is a member of and seeks to represent a Nationwide Class, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3), defined as:

> All Capital One customers within the United States whose Capital One consumer bank account(s) were debited via one or more unauthorized transactions using Zelle and were not fully reimbursed by Capital One.

101. Excluded from the Nationwide Class are Defendant's officers, directors, and employees; any entity in which Defendant have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Further excluded from the Nationwide Class are members of the judiciary to whom this case is assigned, their families, and members of their staff.

102. Plaintiff reserves the right to modify the proposed class definitions, including but not limited to expanding the class to protect additional individuals and to assert additional sub-classes as warranted by additional investigation.

103. The proposed Nationwide Class meet the criteria for certification under Rule 23(a), (b)(2) and (b)(3).

104. **Numerosity:** The members of the Nationwide Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, on information and belief, the Nationwide Class consists of thousands of individuals nationwide.

105. **Commonality:** There are questions of law and fact common to the Nationwide Class, which predominates over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation.

106. Whether Plaintiff and the Class Members lost money that was unlawfully

transferred from their account via Zelle;

a. Whether the transactions at issue were Unauthorized EFTs, by way of a third party fraudulently obtaining access to Plaintiff's and the Class Members' accounts, making them errors subject to EFTA's remedial provisions, including Regulation E;

b. Whether Defendant violated EFTA by failing to adequately investigate the unauthorized transactions of Plaintiff and the Class Members;

c. Whether Defendant violated EFTA by failing to provisionally credit the accounts of Plaintiff and the Class Members within 10 days of the transaction being disputed;

d. Whether Defendant violated EFTA by failing to correct errors resulting from unauthorized transactions on the accounts of Plaintiff and the Class Members;

e. Whether Plaintiff and the Class Members are entitled to damages, including treble damages, maximum statutory damages, costs, fees and injunctive relief under the EFTA;

f. Whether the conduct of Defendant constitutes a breach of contract and the implied covenant of good faith and fair dealing;

107. **Typicality**: Plaintiff's claims are typical of those of other members of the Nationwide Class because Plaintiff and Class Members were victims of unauthorized transfers of funds from their Capital One account, through the Capital One website, or through the Capital One or Zelle mobile app. After disputing that unauthorized transaction, Plaintiff and Class Members were informed by Defendant that the unauthorized transaction(s) would not be reversed or repaid.

108. **Adequacy of Representation**: Plaintiff will fairly and adequately represent and protect the interests of members of the Nationwide Class. Plaintiff and his counsel have no

conflicts of interest with the proposed Class. Plaintiff's Counsel are competent and experienced in litigating consumer class actions.

109. **Predominance**: Defendant has engaged in a common course of conduct toward Plaintiff as well as the members of the Nationwide Class, in that all were induced into using Capital One's mobile app and online banking, that resulted in unauthorized withdrawals on their Capital One accounts using Zelle. The common issues arising from Defendant's conduct affecting members of the Nationwide Class set out above predominate over any individual issues, such as damages. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

110. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most members of the Nationwide Class would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual members of the Nationwide Class would create a risk of inconsistent or varying adjudications with respect to individual members of the Nationwide Class, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

111. Defendant has acted on grounds that apply generally to the Nationwide Class, so that class certification is appropriate.

112. All Members of the proposed Nationwide Class are readily ascertainable. Defendant has access to consumer reporting of fraudulent and/or unauthorized transactions on their books and records, which they are required by law to maintain accurately. Using this

information, Class Members easily can be identified and ascertained for the purpose of providing notice.

113. **Notice**: Plaintiff anticipates providing direct notice to the members of the Nationwide Class for purposes of class certification, via U.S. Mail, email, and/or other electronic means, based upon Defendant's records.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of The Electronic Fund Transfer Act ("EFTA")

114. Plaintiff realleges and incorporates herein by reference the allegations contained in all preceding paragraphs, and further allege as follows:

115. The Electronic Fund Transfer Act ("EFTA") and Regulation E apply to electronic fund transfers that authorize a financial institution to debit or credit a consumer's account. 12 C.F.R. § 1005.

116. The primary objective of EFTA is "the protection of individual consumers engaging in electronic fund transfers and remittance transfers." 12 C.F.R. § 1005.1(b). Financial institutions have error resolution obligations pursuant to Regulation E in the event that a consumer notifies the financial institution of an error. 12 C.F.R. § 1005.11.

117. Capital One is a financial institution. 12 C.F.R. § 1005.2(i).

118. Pursuant to the EFTA, an error includes "an unauthorized electronic fund transfer." *Id.* § 1693f(f).

119. Electronic Fund Transfer ("EFT") is any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's

account. 12 C.F.R. 1005.3(b)(1).

120. Accordingly, Regulation E applies to any P2P or mobile payment transactions that meet the definition of EFT. 12 C.F.R. 1005.3(b)(1)(v); Comment 3(b)(1)–1ii.

121. Unauthorized EFTs are EFTs from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit. 12 C.F.R. 1005.2(m).

122. According to the CFPB and FDIC, when a third party fraudulently induces a consumer into sharing account access information that is used to initiate an EFT from the consumer's account, that transfer meets Regulation E's definition of an unauthorized EFT. In particular, Comment 1005.2(m)–3 of Regulation E explains that an unauthorized EFT includes a transfer initiated by a person who obtained the access device from the consumer through robbery or fraud. As such, when a consumer is fraudulently induced into sharing account access information with a third party, and a third party uses that information to make an EFT from the consumer's account, the transfer is an unauthorized EFT under Regulation E.14.

123. Here, criminals used Plaintiff's and Class Members' Capital One online account or mobile app to make unauthorized EFTs from Plaintiff's and Class Members' Capital One bank accounts.

124. After the unauthorized EFTs were made, the EFTs appeared on the bank statements of Plaintiff and Class Members.

125. Plaintiff and Class Members notified Defendant of these errors within sixty (60) days of their appearances on the accounts of Plaintiff and Class Members.

126. After receiving notice of the unauthorized EFTs on Plaintiff' and other Class

Members' accounts, Defendant erroneously concluded that an unauthorized transfer did not occur.

127. Capital One did not make a good faith investigation of the alleged error and did not have a reasonable basis for believing that the consumer's account was not in error in violation of 15 U.S.C. § 1693f.

128. Capital One knowingly and willfully concluded that the Plaintiff and Class members accounts were not in error when such conclusion could not reasonably have been drawn from the evidence available to the financial institution at the time of its investigation.

129. Defendant knowingly and willfully failed to fulfill their obligations to investigate Plaintiff's unauthorized transactions and instead summarily concluded that the transfers of funds via Zelle on accounts of Plaintiff and Class Members were not in error when such conclusions could not reasonably have been drawn from the evidence available to the financial institutions at the time of the investigation. 15 U.S.C. § 1693f(e)(2).

130. Defendant did not investigate and determine whether an error has occurred and report or mail the results of such investigation and determination to the consumer within ten (10) business days. 15 U.S.C. § 1693f(a).

131. Defendant did not provisionally recredit the consumers account after ten days after receipt of notice of error to investigate, for the amount alleged to be in error pending an investigation. § 1693f(c).

132. Defendant refused to completely reverse or refund funds to Plaintiff and Class Members consistent with their obligations under Regulation E, § 1005.6.

133. As a direct and proximate result of the conduct of the Bank, Plaintiff and Class Members were unable to reclaim funds that were fraudulently taken from their accounts within

the authorized period for error resolution, and have been damaged thereby.

134. As such, Plaintiff and Class Members are each entitled to (i) actual damages sustained by the consumer; (ii) treble damages; (iii) the lesser of $500,000.00 or one percent (1%) of the net worth of Capital One; (iii) reasonable attorneys' fees and costs; and (iv) injunctive relief to prohibit future unlawful conduct and compliance with the EFTA. 15 U.S.C. §§ 1693f(e)(2), and 1693m(a)(2)(B)(3).

SECOND CAUSE OF ACTION

Breach of Contract

135. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

136. Capital One breached its promises and the terms of its contract with consumers as described herein.

137. Plaintiff and members of the Class contracted with Capital One for checking account services, including mobile banking services, as embodied in the express statements, promises, and the Checking Account Agreement and Electronic Funds Transfer Statement (the "Agreement").

138. Specifically, the Agreement states that:

> Liability for Unauthorized Transfers:
>
> A. We have decided not to impose any liability on you even though the law says we could (up to $50)….if you contact us within two (2) business days after you learn of the loss or unauthorized use.

138. Further, the contract states that even if the bank is not promptly notified, the consumer is only liable when Capital One proves that it could have prevented the losses. The Agreement states:

> . . . .

B. If you do NOT tell us within two (2) business days and we can prove that we could have prevented the loss had you contacted us, you could lose as much as $500.00.

C. If your statement shows transfers that you did not make and you do NOT contact us within sixty (60) days after the statement was made available to you, you may not get back any money lost after the sixty (60) days if we can prove that your contacting us would have prevented those losses.

138. Capital One breached this Agreement by imposing liability on its customers.

139. Capital One breached its express statements and promises that Capital One 's mobile banking was 'secure' and 'safe', that Capital One would be protect Plaintiff and Class Members from fraud, that Plaintiff and Class members would not be liable for unauthorized transactions, and that Capital One would comply with the EFTA and Regulation E.

140. Plaintiff and members of the Classes have performed all of the obligations imposed on them pursuant to the Agreement.

141. Plaintiff and Class Members suffered damages as a result of the Defendant's breach of contract.

142. Accordingly, Plaintiff and Class Members are entitled to damages, including the loss of money via unauthorized Zelle transfers, and any corresponding fees, interest, and charges.

THIRD CAUSE OF ACTION

Breach of the Implied Covenant of Good Faith and Fair Dealing

143. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

144. Capital One breached its promises and the terms of its contract with consumers as described herein.

145. Further, an implied covenant of good faith and fair dealing governs every contract. The covenant of good faith and fair dealing constrains Defendant Capital One's discretion to abuse self-granted contractual power.

146. This contract was subject to an implied covenant of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual duties—both explicit and fairly implied—and not to impair the rights of other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the covenant that Defendant would act fairly and in good faith in carrying out its contractual obligations to reimburse Plaintiff and Class Members for unauthorized transactions if timely reported.

147. Defendant breached the implied covenant of good faith and fair dealing when it failed to fairly investigate reported unauthorized transactions made via Zelle, failed to reimburse accountholders for unauthorized transactions incurred via Zelle, and adopted policies and procedures that contradicted its contractual obligations.

148. Capital One, in bad faith, dishonestly, and intentionally breached the Agreement by knowingly creating policies to deny consumers legitimate claims for unauthorized transfers, refusing to perform a reasonable investigation related to Zelle transfers, and refusing to refund money for unauthorized transactions that were promptly reported by consumers. Moreover, Capital One did not provisionally credit consumers' accounts while it was investigating the claim, as promised in the contract.

149. Each of Defendant's actions were done in bad faith and were arbitrary, dishonest, and capricious.

150. Plaintiff and members of the Classes have performed all of the obligations imposed on the pursuant to the Online Banking Agreement.

151. Accordingly, Plaintiff and Class Members have been injured as a result of Defendant's breach of contract and breach the covenant of good faith and fair dealing and are entitled to actual damages and punitive damages, including the loss of money via unauthorized Zelle transfers, and any corresponding fees, interest, and charges.

FOURTH CAUSE OF ACTION

Negligence

152. Plaintiff realleges and incorporates herein by reference the allegations contained in all preceding paragraphs, and further alleges as follows:

153. Capital One owed Plaintiff and Class Members at least a duty to take reasonable steps to safeguard their financial information and protect their financial accounts from malicious third parties, to adequately warn of known risks and/or dangers associated with its Consumer Checking and Savings Accounts, including the online banking and mobile application, and to properly investigate disputed transactions initiated via Zelle.

154. Defendant breached its obligations to Plaintiff and Class members and were otherwise negligent and/or reckless by at least:

a. Failing to maintain adequate data security measures to prevent or reduce the risk of disclosure of the personal information and to protect Plaintiff and Class Members money.

b. Failing to adequately protect Plaintiff and Class Members from the risks of

unauthorized transactions and fraud via Zelle on Capital One's mobile banking website and application.

c. Failing to properly warn Plaintiff and Class Members of the risks and/or dangers associated with Capital One Mobile Banking, the risks or dangers associated with Zelle, or informing consumers about the Zelle related scams;

d. Failing to adequately investigate and document findings from the investigations of EFT disputes of the unauthorized transactions made on the accounts of Plaintiff and Class Members, using the Capital One/Zelle payment platform;

e. Failing to take appropriate steps to avoid unauthorized transactions through the Capital One Mobile Banking and/or application in response to known scams and continuing with business as normal;

f. Failing to implement appropriate and sufficient safeguards against scams of the nature alleged in the Complaint in light of the knowledge that those scams have been rampant across the country;

g. Permitting scammers to use Zelle to siphon funds from the accounts of Plaintiff and Class Members;

h. Failing to reverse unauthorized transactions pursuant to Regulation E error resolution requirements following disputes of Plaintiff and Class Members despite Defendants' knowledge that said transactions were unauthorized as part of a scam that is well- known to Defendants; and

i. Failing to permanently reverse unauthorized transactions upon a sufficient showing by Plaintiff and Class Members that said transactions were unauthorized

154. As a direct and proximate result of Defendants' breach, Plaintiff and Class

Members lost money from their Capital one accounts.

155. Plaintiff and Class Members are entitled to damages for their continuing and increased risk of fraud and for their loss of money.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, prays for relief in this Complaint as follows:

A. Class certification of this action, including appointment of Plaintiff as Class Representative; and appointment of Plaintiff's attorneys as Class Counsel;

B. An award of actual damages, in an amount to be determined at trial;

C. An award of treble damages against Capital One pursuant to the EFTA;

D. An award of the lesser of $500,000.00 or one percent (1%) of the net worth of Capital One pursuant to the EFTA;

E. An award of Punitive Damages;

F. Injunctive and other equitable relief against Defendant;

G. Costs of Suit;

H. Pre- and post-judgment interest;

I An award of reasonable attorneys' fees pursuant to the EFTA; and

J. Any other relief the Court may deem just and proper.

Plaintiff hereby demands a jury trial on all issues so triable.

Dated: April 26, 2023

Respectfully submitted,

/s/ Heather Whitaker Goldstein
Heather Whitaker Goldstein
VA State Bar No 41480
David M. Wilkerson*
THE VAN WINKLE LAW FIRM
11 North Market Street
Asheville, NC 28801
Phone: 828-258-2991
Fax: 828-257-2767
Email: hgoldstein@vwlawfirm.com
Email: dwilkerson@vwlawfirm.com

Andrew J. Shamis*
Edwin E. Elliott*
SHAMIS & GENTILE, P.A.
14 NE First Avenue, Suite 705
Miami, Florida 33132
Telephone: 305-479-2299
ashamis@shamisgentile.com
edwine@shamisgentile.com

Jeffrey D. Kaliel*
Sophia Goren Gold*
KALIELGOLD PLLC
1100 15th Street NW, 4th Floor
Washington, D.C. 20005
Telephone: (202) 350-4783
jkaliel@kalielpllc.com
sgold@kalielgold.com

Scott Edelsberg*
Christopher Gold*
EDELSBERG LAW, PA
20900 NE 30th Ave, Suite 417
Aventura, Florida 33180
Telephone: 305-975-3320
scott@edelsberglaw.com
chris@edelsberglaw.com

**Pro Hac Vice forthcoming*

Counsel for Plaintiff and the Proposed Class